UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/736,718	12/12/2000	David Michael Kurn	20206-031 (P00-3015)	8323

7590 06/30/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/736,718	KURN ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the application filed on 12/12/2000.

2. Claims 1-44 are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-44 are rejected under 35 U.S.C. 102(b) as being anticipated by Brennan et al, US Patent No. 5675649, hereinafter "Brennan".

5. As per claims 1, 8, 38, and 43, Brennan teaches "A cryptographic system in a computer system, said cryptographic system comprising: at least one server; a database, said database constructed and arranged to contain sensitive information, said database responsive to signals from one of said at least one server" in (Col 1 lines 10-27); "a key repository process on one of said at least one server, said key repository having two master keys, said two master keys constructed and arranged to manage information in said database, said key repository further constructed and arranged to authorize access to said sensitive information in said database" in (Col 1 lines 10-27, Col 3 lines 55-60); "at least one operator, said at least one operator having access to a

first of said master keys" in (Col 5 lines 25-35, locking key); "the at least two owners, each of said owners having a portion of a second of said master keys; wherein said at least operator and at least one of said owners are required to start said key repository process" in (Col 5 lines 27-35, Col 13 lines 45-55, Master key).

6. As per claims 2 and 39, Brennan discloses "A cryptographic system as in claims 1 and 38, wherein said operator is enabled to assert that said computer system is genuine" in (Col 6 lines 13-40).

7. As per claims 3, 31, and 40, Brennan discloses "A cryptographic system as in claims 2, 10, and 39 wherein if said operator asserts that said computer system is genuine, then said computer system is enabled to unlock and expose a set of cryptographic credentials that can be used by said key repository" in (Col 8 lines 20-35).

8. As per claims 4 and 32, Brennan discloses "A cryptographic system as in claims 1 and 10, wherein said first master key is an integrity key" in (Col 17 lines 25-40).

9. As per claims 5 and 33, Brennan discloses "A cryptographic system as in claims 1 and 10, wherein said first master key is a protection key" in (Col 5 lines 33-35).

10. As per claims 6 and 34, Brennan discloses " A cryptographic system as in claims 1 and 10, wherein said second master key is an integrity key" in (Col 6 lines 1-5).

11. As per claims 7 and 35, Brennan discloses "A cryptographic system as in claims 1 and 10, wherein said second master key is a protection key" in (Col 6 lines 1-5).

12. As per claims 9, 37, and 44, the rejection basis of claim 1 is incorporated. Brennan discloses "A cryptographic system as in claims 8, 36, and 43 wherein said second master key is assembled from a set of secrets that are split among a plurality of owners according to the Bloom-Shamir methodology" in (Col 1 lines 45-55)

13. As per claim 10, Brennan discloses "A cryptographic system in a computer system, said cryptographic system comprising: at least one server; a database, said database constructed and arranged to contain sensitive information, said sensitive information including authentication information for at least one operator and at least two owners, said database responsive to signals from one of said at least one server" in (Col 1 lines 10-27); "a key repository process on one of said at least one server, said key repository having two master keys, said two master keys constructed and arranged to manage said sensitive information in said database, said key repository further constructed and arranged to retrieve said authentication information from said database" in (Col 1 lines 10-27, Col 3 lines 55-60); "wherein one of said operators authenticates himself, and at least one owner authenticates himself in order for said key

repository process to restart" in (Col 13 lines 45-55).

14. As per claim 11, Brennan discloses "A cryptographic system as in claim 10, wherein said one or more of said master keys is exposed upon restart of said key repository" in (Col 13 lines 45-55).

15. As per claim 12, Brennan discloses "cryptographic system as in claim 10, wherein at least one of said owners must approve all changes to said database that affect the security of said computer system" in (Col 13 lines 45-55).

16. As per claim 13, Brennan discloses "cryptographic system as in claim 10, wherein at least one of said owners must approve the addition of an owner" in (Col 11 lines 63-66).

17. As per claim 14, Brennan discloses "cryptographic system as in claim 10, wherein at least one of said owners must approve the addition of an operator" in (Col 11 lines 63-66).

18. As per claim 15, Brennan discloses " cryptographic system as in claim 10, wherein at least one of said owners must approve the addition of an owner and an operator" in (Col 11 lines 63-66).

19. As per claim 16, Brennan discloses " cryptographic system as in claim 10, wherein at least one of said owners must approve the removal of an owner" in (Col 11 lines 63-66).

20. As per claim 17, Brennan discloses " cryptographic system as in claim 10, wherein at least one of said owners must approve the removal of an operator" in (Col 11 lines 63-66).

21. As per claim 18, Brennan discloses " cryptographic system as in claim 10, wherein at least one of said owners must approve the removal of an owner and an operator" in (Col 11 lines 63-66).

22. As per claim 19, Brennan discloses " cryptographic system as in claim 10, wherein at least two of said owners must approve the addition of an owner" in (Col 11 lines 63-66, Col 13 lines 45-55).

23. As per claim 20, Brennan discloses " cryptographic system as in claim 10, wherein at least two of said owners must approve the addition of an operator" in (Col 11 lines 63-66, Col 13 lines 45-55).

24. As per claim 21, Brennan discloses " cryptographic system as in claim 10, wherein at least two of said owners must approve the addition of an owner and an

operator" in (Col 11 lines 63-66, Col 13 lines 45-55).

25. As per claim 22, Brennan discloses " cryptographic system as in claim 10, wherein at least two of said owners must approve the removal of an owner" in (Col 11 lines 63-66, Col 13 lines 45-55).

26. As per claim 23, Brennan discloses " cryptographic system as in claim 10, wherein at least two of said owners must approve the removal of an operator" in (Col 11 lines 63-66, Col 13 lines 45-55).

27. As per claim 24, Brennan discloses " cryptographic system as in claim 10, wherein at least two of said owners must approve the removal of an owner and an operator" in (Col 11 lines 63-66, Col 13 lines 45-55).

28. As per claim 25, Brennan discloses "cryptographic system as in claim 10, wherein at least one of said owners must approve a change in the minimum number of owners required to restart said key repository" in (Col 11 lines 63-66, Col 13 lines 45-55).

29. As per claim 26, Brennan discloses " cryptographic system as in claim 10, wherein at least two of said owners must approve a change in the minimum number of owners required to restart said key repository" in (Col 11 lines 63-66, Col 13 lines 45-

55).

30. As per claim 27, Brennan discloses " cryptographic system as in claim 10, wherein at least one of said owners must approve a change in the minimum number of owners required to restart said key repository" in (Col 11 lines 63-66, Col 13 lines 45-55).

31. As per claim 28, Brennan discloses " cryptographic system as in claim 10, wherein at least two of said owners must approve a change in the minimum number of owners required to restart said key repository" in (Col 11 lines 63-66, Col 13 lines 45-55).

32. As per claim 29, Brennan discloses " cryptographic system as in claim 10, wherein at least one of said owners must approve a change in the approval count" in (Col 11 lines 63-66, Col 13 lines 45-55).

33. As per claim 30, Brennan discloses " cryptographic system as in claim 10, wherein at least two of said owners must approve a change in the approval count" in (Col 11 lines 63-66, Col 13 lines 45-55).

34. As per claim 36, Brennan discloses " cryptographic system as in claim 10 wherein said second master key is assembled from a set of secrets that are split among a plurality of owners" in (Col 5 lines 30-35).

Double Patenting

35. The non-statutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

36. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

37. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

38. Claims 1-44 of the instants application No. 09736718, hereinafter '718, are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-12, 14-27, and 29 of copending Application No. 09735087, hereinafter '087. Although the conflicting claims are not identical, they are not patentably distinct from each other because as follow:

39. The instants application '718:

Exemplary Claim 1 recites:

> **(1)** A cryptographic system in a computer system, said cryptographic system comprising: at least one server; a database, said database constructed and arranged to contain sensitive information, said database responsive to signals from one of said at least one server; a key repository process on one of said at least one server,
>
> **(2)** said key repository having two master keys,
>
> **(3)** said two master keys constructed and arranged to manage information in said database, said key repository further constructed and arranged to authorize access to said sensitive information in said database;

(4) at least one operator, said at least one operator having access to a first of said master keys;

(5) and the at least two owners, each of said owners having a portion of a second of said master keys; wherein said at least operator and at least one of said owners are required to start said key repository process"

40. The copending application '087:

Exemplary Claim 1 recites:

(1) A cryptographic system in a computer system, comprising: a database, the database configured to contain sensitive information; at-least a key repository process operating in the computer s System;

(2) two or more master keys of which at least one master key is a most-secure master key and requiring a multi-part construction to be exposed,

(5) the multi-part construction requiring information from at least two most-secure key owners for the most-secure key to be exposed,

(3) the most-secure master key providing protection to the sensitive information,

(6) relative to the at least one most-secure master key each of the remaining one or more master keys is a less-secure master key and requiring construction from fewer parts to be exposed, the at least one

most-secure master key can be used for detecting tampering of any less secure master key;

(7) and means for cryptographically linking one or more of the at least one most secure master key with one or more less-secure master keys such that any tampering of the one or more less-secure master keys can be detected.

41. As underlined above, the feature **(1)** of both applications recites the exact claim language.

However, The limitations **(2), (3),** and **(5)** in '718 claim the master keys, and a method of implementing the master keys in the invention. The limitations **(2), (3),** and **(5)** in '087 claim the two master keys, a method of implementing the two master keys in the invention, and further construction of the master keys. It is clearly that the limitations **(2), (3),** and **(5)** in instant application '718 would be obvious over the limitation **(2), (3),** and **(5)** in the copending application '078, because the method and system of implementing the master keys claimed in '718 invention provide a clear evidence that the construction master key with the strong security feature claimed to protect the sensitive information in the '087 invention could be necessary for such environment in '718. Further, the limitations **(6)** and **(7)** in '087 are not in '718. Nonetheless, those limitations **(6)** and **(7)** further are claiming the detail construction of the master keys. Therefore, it is clearly that claims 1-10 and 38 in '718 are obvious over the exemplary claim

1 in '078, and clearly claim 1 is a set and the exemplary claims 1 are the subset of the set.

42. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Georgia-Pacific Corp. v. United States Gypsum Co., 195 F.3d 1322, 1326, 52 USPQ2d 1590, 1593 (Fed. Cir. 1999). Second, the court determines whether the differences in subject matter between the two claims render the claims patentably distinct. Id. at 1327, 52 USPQ2d at 1595. A later claim that is not patentably distinct from an earlier claim in a commonly owned patent is invalid for obvious-type double patenting. In re Berg, 140 F.3d 1428, 1431, 46 USPQ2d 1226, 1229 (Fed. Cir. 1998). A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

43. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Patent Examiner

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100